REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of March 29, 2004 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due.

In paragraph 3 of the Office Action, claims 1-3, 4, 16-21, and 23 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,548,647 to Naik, *et al.* (Naik). In paragraph 4, claims 4 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Naik in view of U.S. Patent No. 5,719,560 to Watkins (Watkins). In paragraph 5, claims 5-15 and 24-36 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Naik in view of Watkins, in further view of Coteus.

In response, Applicants have amended the claims to replace the terms "user-identifier" with the terms "authorizing data" to clarify that the authorizing information entered into a security device can be any identification code that can be used to provide access to a publicly positioned device, as shown in FIG. 1. Support for this clarification can be found at page 20, lines 5-8, at page 3, lines 2-5, in FIG. 4 and 5, and throughout the Applicants' specification.

Applicants have also amended the claims to replace the terms "random data" with the terms "obscuring data" to clarify that the data is used to obscure the authorizing data from on-lookers when the data is entered in public. That is, the term random as used by the Applicants denotes data that can not be predicted with anything like certainty. Random data is unpredictable, meaning data that onlookers cannot predict for purposes of distinguishing the authorizing data from a combination of authorizing data and obscuring (random) data. Support for this amendment can be found at page 15, line 22 to page 16, line 13, at page 18, line 16 to page 19, line 7, and at page 19, lines 21-28.

Applicants have amended claims 1 and 19 to clarify that obscuring data is repudiated or ignored for purposes of authorizing access. The device is therefore authorized based upon the authorizing data only. Applicants believe that the authorizing and repudiating steps are more descriptive than the previously utilized discarding step. Support for the amendment can be found in FIG. 5 and throughout the Applicants' specification.

Applicants have added claims 37-39 to clarify that an input device and an authorizing engine that grants access to use the device can be distributed. Additionally, the inputted obscuring data need not be conveyed from the input device to the remotely located authorizing engine. Transport of the authorizing data can occur via a secure or encoded channel. Support for these dependent claims can be found in FIG. 4, FIG. 5, FIG. 7A, and/or FIG. 7B. Additionally, the basis for these claims is evident in the ATM, calling card, and the IVR examples presented within the Applicants specification.

Applicants have also added claims 40 and 41, supported by FIG. 1, FIG. 2, and FIG. 3. No new matter has resulted from these amendments.

Prior to addressing the rejections on the art, a brief review of the Applicants' invention is appropriate. The Applicants have invented a method, apparatus, and system for securing authorizing data from observation. Specifically, users often must interact with machines that require user authentication. For example, uses provide calling card identification numbers, credit card numbers, debit card pin numbers, and other authorizing data to interact with machines. Often, the interactions take place in public, where entry of the authorizing data can be observed by onlookers. The onlookers can thereafter dishonestly utilize the observed authorizing data to interact with machines as if the onlookers were authorized users. Results of these unauthorized accesses can be extremely expensive to the authorized users and/or the entity or entities restricting access of the machine to the authorized user.

To prevent unauthorized access gleaned via public observation, obscuring data can be entered along with the authorizing data. That is, additional information that is not part of the authorizing data can be entered to obscure the content of the authorizing data. The machine can discard, repudiate, or ignore the obscuring data when authorizing the user. Accordingly, the obscuring data is bogus data used only to obscure the authorizing data from public viewing.

In one embodiment, prompts can alternate the obscuring data and the authorizing data thereby causing observable input to consist of a combination of obscuring data and authorizing data. The placement of obscuring data within the combination can vary from interaction to interaction so that no easily discernable pattern exists that would permit an observer to separate obscuring data from authorizing data.

Referring to claim 1 and claim 19, the Applicants claim the steps of:

> authorizing the user to utilize the publicly positioned device based upon the authorizing data; and,
> repudiating the obscuring data during the authorizing step.

Applicants authorize use of a device based upon authorizing data and not based upon the obscuring data. That is, the obscuring data exists to obscure the authorization data from observing entities. The obscuring data is not part of the authorizing process. Naik functions in a fundamentally different manner and does not teach the claimed limitations of the authorizing and repudiating steps.

Naik teaches a voice based security system that utilizes vocal characteristics to confirm a users' identity. In order to prevent unauthorized users to gain access to a secured device, Naik teaches that an arbitrary phrase should be emitted that the speaker desiring access to the secured device must repeat. The speaker's vocal characteristics for the repeated phrase are used during the authorization process. The theory behind Naik is that traditional security techniques can be circumvented by playing previously recorded phrases into a microphone. Since the vocal characteristics of Naik are extracted from a spoken phrase that cannot be known ahead of time, previously recorded phrases cannot be used to circumvent the security measures of the secured device.

Naik fails to teach prompting for obscuring data. Notably, obscuring data (often called random data and/or randomly selected data in the specification) is data used to "mask the entry of a user-identifier (or the authorizing data) which would be otherwise publicly viewable in the absence of the present invention." as noted at page 7, lines 12-13. An example of obscuring data is provided in the context of an ATM machine at page 15, line 22 to page 16, line 13 of the Applications specification. Another example of obscuring data is provided at page 18, line 16 to page 19, line 7. Still another example is provided at page 19, lines 21-28.

In contrast to the obscuring data, Naik teaches the prompting for an identification code and a statement, as described at column 5, lines 7-28. The statement is used during the authentication process and not repudiated or discarded. The vocal characteristics extracted from the statement and are used to verify the speaker's identity, as noted at column 7, lines 26-36. The

authorizing process is dependent upon both the identification code and the statement, as illustrated in FIG. 2 of Naik. Because Naik fails to teach obscuring data that is discarded for authorizing purposes, Naik fails to anticipate the Applicant's invention. Accordingly, the 35 U.S.C. § 102(b) rejections to claims 1-3, 5, 16-21, and 23 should be withdrawn, which action is respectfully requested.

Referring to claims 4 and 22, Applicants assert that the claimed invention is patentable over Naik in view of Watkins. Naik fails to teach a security methodology based upon prompting a user for obscuring data that is repudiated during an authorizing step. That is the obscuring data is "dummy data" not used to authorize access to a secure device. Naik provides no teachings relating to prompting for "dummy data" that is not used within an authorizing process. Instead, use of the speech statements is essential for the security methodology of Naik, as illustrated in FIG. 2. Watkins fails to cure this deficiency. Watkins teaches using cue-sets instead of passwords. Watkins provides no teachings relating to obscuring data.

As neither Naik, Watkins, nor a combination thereof teach or suggest the authorizing and repudiating steps of the applicants invention (that rely upon obscuring data not used when authoring access to a device), the 35 U.S.C. § 103(a) rejections to claims 4 and 22 should be withdrawn, which action is respectfully requested.

Referring to claims 6-15 and 24-36, the Examiner has rejected these claims under 35 U.S.C. § 103(a) as being unpatentable over Naik, in view of Watkins, in further view of Coteus. Coteus, however, fails to cure the previously mentioned deficiencies of Naik-Watkins. Coteus teaches a secure viewing system involving glasses and electronic shutters. Coteus provides no teachings relating to prompting a user for obscuring data, then repudiating received obscuring data during an authorizing step.

As neither Naik, Watkins, Coteus, nor a combination thereof teach or suggest the authorizing and repudiating steps of the applicants invention, the 35 U.S.C. § 103(a) rejections to claims 6-15 and 24-36 should be withdrawn, which action is respectfully requested.

The Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. The Applicants request that the Examiner call the undersigned if

clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: 29 June 2004

Gregory A. Nelson, Registration No. 30,577
Kevin T. Cuenot, Registration No. 46,283
Brian K. Buchheit, Registration No. 52,667
AKERMAN SENTERFITT
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000